WHAT IS CLAIMED IS:

1. An apparatus for facilitating the high speed transfer of data to authorized users over the internet, the apparatus comprising:

a plurality of host machines for running a plurality of processes;

at least one secure communication link between the host machines;

a file storage system having a storeroom area and a customer account area with a hard linking capability there between;

a firewall with at least one secured host machine residing on the secured side of the firewall; and

a customer account database located on the secured host machine and accessible by a secured communication link through the firewall.

2. The apparatus of Claim 1, wherein the at least one secure communication link utilizes a protocol for the exchange of arbitrary sized packets of ascii data, delimited by carriage return and newline boundary markers.

3. The apparatus of Claim 2, wherein at least one secure communication link enhances the protocol by utilizing DES encryption with N DES keys, and a method for securely

passing the DES keys comprising the steps of:

(i) finding the port number P used for the connection;

(ii) computing a value I = P modulo N; and

(iii) using I as the index into the N keys, and using the DES key residing at index I to encrypt and decrypt the data stream.

4. The apparatus of Claim 3, wherein the DES encryption creates a cypher string, and a filter is applied to render the cypher string at least 7-bit safe.

5. The apparatus of Claim 1, wherein the hard linking capability includes a change root command.

sub a2

6. The apparatus of Claim 1, wherein the secured link through the firewall utilizes tobj protocol.

7. The apparatus of Claim 1, wherein at least one host machine runs a web server process and at least one separate host machine runs an ftp server process, whereby a customer web browser contacts the host machines.

8. A method of facilitating the high speed transfer of data to authorized users over the internet, the method comprising the steps of:

(i) running a web server process on at least one host machine;

(ii) running an ftp server process on a separate host machine;

(iii) establishing a secure communication link between the host machines;

(iv) establishing a hard link between storeroom file storage areas and customer account file storage areas; and

(v) dynamically allocating customer access information from a secured database.

9. The method of Claim 8, wherein step (iii) uses a protocol for the exchange of arbitrary sized packets of ascii data delimited by carriage return and newline boundary markers, and using DES encryption with N keys, step (iii) including the following steps:

(a) finding the port number P used for the connection;

(b) computing an index value I, where I = P modulo N; and

(c) using the DES key residing at index I to encrypt and decrypt the data stream.

10. The method of Claim 9, wherein the DES encryption creates a cypher string, and filtering is applied to render the cypher string at least 7-bit safe.

11. An apparatus for facilitating the high speed transfer of data to authorized users over the internet, the apparatus comprising:

a plurality of host machine means for running a plurality of processes;

at least one secure means for communicating between the host machines;

a file storage means having a storeroom area and a customer account area with a means for securely hard linking between the areas;

a firewall means for providing security between machines; with at least one secured host machine means residing on the secured side of the firewall;

a means for databasing customer accounts located on the secured host machine means and accessible by a secured means for communicating through the firewall.

add A3